Office Action Summary	Application No.	Applicant(s)	
	09/931,338	VATANEN ET AL.	
	Examiner	Art Unit	
	Eleni A Shiferaw	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 February 1999*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-18* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-18 are presented for examination.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Khan et al. (Khan, US Patent No.: 6,401,206 B1) in view of Scheibel, Jr. et al. (Scheibel, US Patent No.: 6,212,240 B1), and in further view of Rittle (US Patent No.: 6,173,431 B1).

4. As per claim 1, Khan teaches a method for transmitting in encrypted form, from a sender to a receiver, an initially unencrypted message so as to enable, through encryption, verification of authenticity of the sender and of integrity of contents of the message, comprising the steps of:

Khan teaches at least one of encrypting and signing of the data section using an encryption method to enable reliable identification of the sender and the receiver of the encrypted message (Col. 6 lines 1-67, Col. 1 lines 7-11)

Khan fail to explicitly teaches the header section of dividing the unencrypted message, adding sender identification data to the header section,

appending the generated check element to the end of the data section,

However Scheibel teaches dividing the unencrypted message to be transmitted into a data section containing the contents of the unencrypted message and a header section (Scheibel '240, Par 3 lines 55-60);

adding sender identification data to the header section (Scheibel '240 Col. 4 lines 1-23);

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Scheibel with in the system of Khan because it would allow the message header to be always transmitted at the lowest modulation rate, to maximize the likelihood of successful transfer of the control information and allow the data blocks to minimize bandwidth consumption. (Col. 4 lines 1-20)

Khan and Scheibel do not explicitly teach appending the generated check element to the end of the data section, and

generating a check element from the content of the message to be transmitted,

However Rittle teaches generating a check element from the contents of the message to be transmitted (Col. 2 lines 22-41, col. 7 lines 38-52);

appending the generated check element to the end of the data section (Col. 9 lines 20-29);

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Rittle with in the system of, the combination of, Khan and Scheibel because it would allow to compare message and if compared message is successful, the receiver accepts the entire information packet, (Col. 4 lines 1-20) and if the compared message is unsuccessful the transmitter transmits an acknowledgment signal indicating that the information packet in its entirety were not correctly received (Col. 5 lines 48-67).

5. As per claim 2, all Khan, Scheibel, and Rittle the subject matter as described above. In addition Khan teaches a method, wherein the check element is generated using a hash function (Col. 2 lines 10-14).

6. As per claim 3, all Khan, Scheibel, and Rittle the subject matter as described above. In addition Khan teaches a method in accordance with claim 1, wherein the encryption method for said at least one of encrypting and signing of the data section comprises a public-private key encryption method (Col. 5 lines 36-49).

7. As per claim 4, all Khan, Scheibel, and Rittle the subject matter as described above. In addition Khan teaches a method in accordance with claim 1, wherein the encryption method for said at least one of encrypting and signing of the data section comprises use of the RSA encryption algorithm (Col. 5 lines 36-49).

8. As per claim 5, all Khan, Scheibel, and Rittle the subject matter as described above. In addition, Khan teaches a method, further comprising the step of adding to the header section an identifier of the encryption method used for said at least one of encrypting and signing of the data section (Khan, col. 4 lines 65-67, col. 5 lines 36-49).

9. As per claim 6, all Khan, Scheibel, and Rittle the subject matter as described above. In addition Khan teaches a method, wherein the sender identification data added to the header

section comprises identification of an owner of a public key to be used to decrypt (Col. 7 lines 1-4) and verify a signature of the encrypted message (Col. 12 lines 19-30, col. 12 lines 49-64).

10. As per claim 7, all Khan, Scheibel, and Rittle the subject matter as described above. In addition Khan teaches a method, wherein said step of at least one of encrypting and signing of the data section comprises signing of the data section with a digital signature (Abstract, Col. 12 lines 1-18).

11. As per claim 8, all Khan, Scheibel, and Rittle the subject matter as described above. In addition Khan teaches a method, wherein said step of at least one of encrypting and signing of the data section comprises signing of the data section using a private key of the sender (Abstract) and the encryption method comprises a public-private key encryption method (Col. 7 lines 1-5).

12. As per claim 9, all Khan, Scheibel, and Rittle the subject matter as described above. In addition Khan teaches a method, wherein said step of at least one of encrypting and signing of the data section further comprises encrypting the signed data section using a public key of the receiver (Col. 4 lines 65-67, col. 5 lines 30-49).

13. As per claim 10, all Khan, Scheibel, and Rittle the subject matter as described above. In addition Khan teaches a method, further comprising the step of decrypting the transmitted encrypted message using a private key of the receiver (Col. 5 lines 53-57).

14. As per claim 11, all Khan, Scheibel, and Rittle the subject matter as described above. In addition Khan teaches a method, further comprising the step of identifying the sender of the transmitted encrypted message by decrypting, after said decrypting of the transmitted encrypted message using the private key of the receiver, the transmitted encrypted message using a public key of the sender (Col. 5 lines 53-57).

15. As per claim 12, all Khan, Scheibel, and Rittle the subject matter as described above. In addition Khan teaches a method, further comprising the step of identifying the sender of the transmitted encrypted message by decrypting the transmitted encrypted message using a public key of the sender (Col. 5 lines 53-57).

16. As per claim 13, all Khan, Scheibel, and Rittle the subject matter as described above. Khan and Scheibel do not explicitly teach check element appended to the data section, However Rittle teaches a method, wherein the integrity of the transmitted encrypted message is verified using the check element appended to the data section (Col. 9 lines 1-29)

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Rittle with in the system of, the combination of, Khan and Scheibel because it would allow to compare message and if compared message is successful, the receiver accepts the entire information packet, (Col. 4 lines 1-20) and if the compared message is unsuccessful the transmitter transmits an acknowledgment signal indicating that the information packet in its entirety were not correctly received (Col. 5 lines 48-67).

17. As per claim 14, all Khan, Scheibel, and Rittle the subject matter as described above. In addition Rittle teaches a method, further comprising the step of requesting, if errors are detected in the contents of the transmitted encrypted message, retransmission of the encrypted message (Col. 1 lines 49-67, col. 9 lines 59-64).

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Rittle with in the system of, the combination of, Khan and Scheibel because it would be more efficient (i.e., much less overhead is consumed in sending an error detection code and retransmitting erroneous data blocks than is required) (Col. 1 lines 49-63)

18. As per claim 15, all Khan, Scheibel, and Rittle the subject matter as described above. In addition Rittle teaches a method, further comprising the step of transmitting an acknowledgement of successful transmission of the encrypted message (Col. 10 lines 15-36).

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Rittle with in the system of, the combination of, Khan and Scheibel because it would indicate that the information packet was correctly received (Col. 10 lines 15-36).

19. As per claim 16, all Khan, Scheibel, and Rittle the subject matter as described above. In addition Rittle teaches a method, further comprising the step of transmitting the encrypted message through a mobile communication system (Col. 4 lines 44-63) The rational for combing are the same as claim 1 above.

20. As per claim 17, all Khan, Scheibel, and Rittle the subject matter as described above. In addition Rittle teaches a method, where the mobile communication system comprises a GSM system (Col. 4 lines 44-63) The rational for combing are the same as claim 1 above.

21. As per claim 18, all Khan, Scheibel, and Rittle the subject matter as described above. In addition Khan teaches a method, wherein said step of at least one of encrypting and signing of the data section being carried out using a mobile station (Col. 4 lines 35-45).

22. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A Shiferaw whose telephone number is 703-305-0326. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Eleni Shiferaw
Art Unit 2136

E. Shiferaw
4/11 2136

for Ayaz Sheikh